Summary of Industry Comments:

Smart Access Common ID Preliminary Requirements Document

Introduction

The General Services Administration (GSA) has been involved in the Smart Access Common ID Project for the past year. The Smart Access Common ID Card program will establish a contract vehicle for use by all Federal agencies to acquire a standard, interoperable employee identification card, from one or more vendors, capable of providing both physical and logical (system/network) access to all Federal employees. The Smart Access Common ID Card will initially focus on providing employee identification and building and network access, but will incorporate additional applications in the future. It will likely include a variety of technologies, among them, integrated circuit chip, magnetic stripe, digitized photo, biometrics, and other media as required by individual agencies.

In an initial phase of this project, a *Preliminary Requirements Document* has been produced and reviewed by government agencies. On May 13, 1999 at the CardTech/SecurTech conference, a GSA held a meeting with industry representatives to present the *Smart Access Common ID Requirements Document*. Industry comments were solicited and the document was posted to the GSA web site. Comments were received from the following companies:

- Datacard Group
- Gemplus
- Kelly, Anderson & Associates
- Morpho
- PriceWaterhouseCoopers
- PRC
- SAIC
- Schlumberger
- Spyrus
- Systems Engineering, INC.
- TECSEC
- 3 GI
- XTEC
- Dreifus Associates, Ltd.

The Common Access Smart Card Advisory Group carefully reviewed industry comments. When necessary, comments were referred to several of the sub-committees of the Common Access Smart Card Advisory Group, including the PKI and the Biometrics Task Forces, for further research and discussion. It is the intent of this document to summarize the comments received by industry and to provide GSA’s response to these comments. Rather than addressing each comment individually, this document will review the key areas of concern to industry. In many cases, the *Smart Access Common ID Card Requirements Document* was revised to reflect changes recommended by industry. However, in some instances, the Advisory Group decided not to alter the requirements document.

Industry comments were broad based, touching on a range of topics. However, the majority of comments can be categorized into the following areas:

- Standards
- Levels of Assurance
- Card Management/Ownership
- Public Key Infrastructure
- Biometrics
- Technology
- Security
- Interoperability
- Business Case

In the sections below, vendor comments in each of these areas will be discussed in greater detail. While the comments varied substantially from vendor to vendor, several common themes emerged from the review:

- **Specificity versus flexibility**. A key theme was the trade-off between specificity and flexibility. While some vendors were concerned about the lack of specificity in various areas (e.g., data structure on card, biometric specifications, etc), others applauded the flexibility provided to individual agencies.

- **Single versus multiple standards.** In the standards arena, some vendors proposed selecting a single standard and mandating compliance to ease achievement of interoperability. Other vendors recommended allowing multiple standards to exist to enable individual agencies to select solutions that conformed to their unique requirements and technical environments.

- **Practicality of/responsibility for interoperability.** A number of vendors indicated that it was impractical at this point in time to mandate interoperability and questioned who would designate responsibility among the teams for achieving interoperability. The impact of various requirements on interoperability pervaded the responses from industry.

- **Importance of supporting emerging technology by not precluding alternative solutions.** Many vendors pointed out the need for flexibility to enable emerging technology to be proposed. GSA, in response, stressed the importance of avoiding any requirements in the document that would preclude any proposed solutions.

- **Need for multiple levels of assurance.** Vendors stressed the importance of accommodating requirements for multiple levels of assurance so as to meet the individual needs of the agencies.

- **Need for common business practices, administrative guidelines, and operating rules for consistent card management.** Several vendors pointed out that the Smart Access Common ID card will require business agreements between agencies who wish to be interoperable with each other. GSA stressed the importance of creating administrative guidelines and sample business agreements to support interoperability once the contract vehicle is in place.

- **Responsibility for certification of applications /assurance of trustworthiness of Certification Authority / Attribute Authority.** Vendors pointed out the importance in a multi-application environment of ensuring the trustworthiness of applications, as well as of

CAs/AAs providing services under the contract vehicle. GSA agreed that such responsibility would be addressed in subsequent administrative guidelines.

Standards

Many of the comments received from industry addressed the specific standards cited in various sections of the document. Several vendors argued that by citing multiple standards, interoperability would be far more difficult to achieve. Additionally, vendors made specific recommendations as to the "open" standards that should be chosen. Different vendors recommended conflicting standards.

While GSA understands the impact of supporting multiple standards on achieving interoperability, the agency regards the objectives of maximizing competition and not precluding any potential solution of paramount importance. Consequently, it has decided to continue to cite multiple standards so that individual agency needs can be met. Agencies to which interoperability is important will have to work out appropriate business arrangements. These agreements must specify agreed upon mutual standards prior to placing task orders under the Smart Access Common ID contract vehicle. GSA welcomes any effort by the industry to address conflicting standards and will incorporate into the document any recommendations that are commonly accepted through this effort.

Several vendors suggested that the *Smart Access Common ID Requirements Document* cite only formal standards and that references be removed to documents that have not undergone the scrutiny of the complete standards process. GSA agrees that it should not mandate conformance to documents for which consensus has not been achieved through the completed standards process. However, certain documents that have not yet achieved the status of formal standards may provide useful guidance for the agencies. Therefore, references to these documents will remain in the requirements document as sources of information, even though conformance with such documents will not be mandated.

Levels of Assurance

The vendor community has agreed with the government that the *Smart Access Common ID Card Requirements Document* should specify multiple levels of assurance. However, a number of vendors disagreed with the suggested levels of security given as examples in the section on interoperability. The Department of Defense (DoD) and the Federal PKI Steering Committee (FPKI) have been working together to define standard levels of assurance to be used throughout the government. To follow the lead of the DoD and FPKI Steering Committee, GSA will base its examples of levels of assurance on the DoD/FPKI model. Thus, the *Smart Access Common ID Card Requirements Document* will be modified to be in conformance with the DoD/FPKI Steering Committee levels of assurance. The existing examples will be removed from the document and be replaced by a reference to the DoD document that specifies these assurance levels.

Card Management/Ownership

In the card management arena, the fundamental issue of specificity versus flexibility was particularly significant, especially when vendors commented on requirements for card initialization and personalization. Some vendors felt that too much detail was specified, while others argued that not enough specifications were provided. Vendors expressed concern that by allowing multiple protocols for loading of cards, interoperability could be impacted. They especially expressed concern that data formats were not provided in the document for storing data on the card or for archiving of data. There was common agreement on the need for an established data dictionary for data to be shared across agencies. Configuration control measures also were suggested.

GSA strongly supports the idea of smart card data fields that comply with government “open standard” data formats maintained in data dictionaries. While GSA understands the concerns of the vendors about the lack of standard data definitions and formats for common data elements across government agencies, it believes it would be impractical to hold up issuance of the RFP until such standards could be developed. GSA would encourage any effort on the part of industry to agree to a common set of demographic data that could be used across agencies. GSA would provide any necessary assistance to support such an industry initiative and would adopt any such standards that were agreed to by industry stakeholders.

Another issue raised by vendors is the ownership of demographic data for the card. GSA maintains that such data would belong to the government, but policies and procedures for handling and securing such data would be incumbent on the individual agencies. Thus, GSA recognizes the importance of developing, in parallel to technical specifications, common business practices, administrative guidelines, and interagency agreements to specify many of the details of the card platform implementation. Additionally, GSA will support the efforts of the individual agencies in agreeing to common configuration management procedures, as well as the establishment of common application libraries, data dictionaries, and other tools to encourage coordinated development efforts.

Public Key Infrastructure (PKI)

A number of comments were received in the area of Public Key Infrastructure (PKI). Many of these issues raised substantial debate within the Common Access Smart Card Advisory Group and were referred to the PKI Task Force. Again, the arguments from vendors were often conflicting and balanced the concept of specificity against flexibility. For example, several vendors pointed out the need for specifying identity proofing requirements. The PKI Task Force opted for flexibility, determining that the identity proofing requirements would vary by agency depending on the level of assurance required for the digital certificate. The Task Force agreed that identify proofing requirements should be determined by individual agencies in conformance with the policies stipulated in the DoD and Federal PKI documents that address levels of assurance. Similar arguments were made for the inclusion of PKI performance benchmarks, which some vendors argued, might vary according to different agency environments, conditions, and requirements. In this case, the PKI Task Force determined that the performance benchmarks provided useful information that should be kept in place as guidelines to be used as agencies saw fit.

Vendors expressed concern about the impact of agency specified validation protocols and certificate formats. While specificity would make interoperability easier, it would hamper unique agency implementations. To vendor concern over the requirement for on-line certificate validation, GSA expressed its expectation that Certificate Authorities be able to respond in some manner to validation requests on-line, whether or not an on-line validation protocol was actually implemented by an agency.

Another area of concern centered on key storage procedures and the use of PKCS #15 compliant data formats. The PKI Task Force determined that there should be separate key pairs for encryption and digital signature and that dual certificates should be required for each separate key pair. Furthermore, the PKI Task Force recommended that key recovery requirements be put in place for the encryption keys but not for the digital signature keys. Solutions that utilize file structures for storage of digital certificates on the card should adhere to PKCS#15 data structures. However, PKCS #15 is but one emerging standard, and thus, this recommendation should not preclude other approaches to storing PKI objects (such as object oriented approaches) that contribute to interoperability requirements. The PKI Task Force agreed with industry comment that key pairs should not be stored in the cardholder database for card replacement. Rather, cards should be reissued with new keys and new digital certificates. The requirements document will be revised to reflect this policy.

The issue of the inclusion of Elliptic Curve technology in the document was particularly controversial. Because FIPS Pub. 186-1 does not specifically address the certification of elliptic curve technology, the PKI Task Force determined that it should not be specifically added to the document. However, it is the intention of the PKI Task Force not to preclude any emerging technology that is approved by the National Institute of Standards and Technology.

Several vendors questioned the specific relationship that this effort has with the ACES program and pointed out that the two efforts were likely to be redundant. The PKI Task Force responded that both efforts were necessary and should be compatible. The ACES program is geared toward the provision of certificates for the general public and has a pricing strategy that may be unacceptable to agencies requiring routine certificate validation transactions for its employees. Consequently, while ACES certificates could be used by some agencies for the Smart Access Common ID Card Program, an alternative should be available for agencies that choose not to use ACES certificates for its employees.

Disagreement among vendors arose over the issue of necessary audit data for PKI transactions. While some vendors felt that detailed auditing was necessary, others were concerned about the practicality of supporting the tremendous amount of audit data that would result from such a requirement. The PKI Task Force determined that the document should be revised to include all of the transactions currently specified with the exception of validation transactions. Furthermore, the requirement for a 30-year archive should be changed to a time period agreeable to each individual agency.

Biometrics

As was the case with PKI, a number of conflicting comments were received in the area of biometrics. Many of these issues raised substantial debate within the Common Access Smart Card Advisory Group and were referred to the Biometric Task Force. A discussion of the key issues and the Biometrics Task Force’s response follows.

The draft requirements document currently limits the use of biometrics to verifying a claimed identity rather than establishing the uniqueness of a claimed identity. However, one vendor suggested that fraudulent enrollees might be able to be deterred if a database of captured biometric templates of failed enrollees be maintained in order to identify such previously rejected enrollees. By using a one-to-many procedure to check against this database, previously rejected enrollees could be prevented from trying to enroll again. Although the Advisory Group thought that such a capability was not likely to be desired by many agencies, the wording of the requirements document will be adjusted to ensure that such a process would not be precluded, should an agency need to implement it.

A number of vendors questioned whether the BioAPI should be cited as the required biometric API as it is not yet finalized. The Biometrics Task Force determined that it appears that the BioAPI is the most widely available and supported biometric API. Other possibilities such as BAPI and HA-API have now merged with BioAPI and will not be supported in the future. However, the requirements document will be revised so as to make clear that conformance with BioAPI is recommended not mandated, since the BioAPI has not been finalized and is not yet in a formal standards process. Yet another suggested approach is to require that implementations be compatible with the BioAPI specification available at the time of implementation.

Another area of controversy surrounded the determination of False Acceptance Rates and False Rejection Rates (FAR/FRR). Vendors pointed out that without mandated testing procedures, it is unlikely that agencies will be able to achieve the desired uniform procedures and comparable results across products. The Biometrics Task Force responded that testing of biometric systems is difficult and that there are no universally accepted procedures for testing or for calculating error rates. Therefore, the Task Force recommends that vendors be required to back up statements about their FAR/FRR rates by describing the methods of the testing, who conducted the testing, how the testing results were gathered and analyzed, and the mathematical methods used to analyze the test results. The requirements document will be revised to require that such documentation be presented and that generally accepted test procedures and analysis methods be used.

The performance standard of 1 sec or less was also highly controversial. Vendors were unsure as to what the 1 second or less referred (i.e., to processing time or to performing an end-to-end transaction that includes data acquisition that is highly application dependent). Furthermore, some vendors were concerned that this standard would preclude certain products. The Biometrics Task Force clarified the meaning of the standard as pertaining to the biometric capture time (i.e., from the time of image offer). The Task Force decided that it should be up to each agency to determine the acceptable time for an end-to-end transaction. It further argued that past experience has shown that end users fail to adopt new technology if it is difficult or awkward to use. Informal testing with users has indicated that any authentication process that takes more than 1 second is undesirable. Therefore, the Task Force decided to leave the standard as it currently is specified in the requirements document.

Equally controversial was the practicality of making attribute certificates mandatory. Vendors pointed out that the use of the attribute certificate would require an infrastructure that could be highly expensive to establish and maintain. The Biometrics Task Force suggested that the goal when using attribute certificates was to leverage off of current or planned infrastructures (such as those being developed for PKI) and not to create the need for a separate infrastructure just for biometric data. Furthermore, the Biometric Task Force maintained that the agencies requiring high security would not be willing to adopt an approach that provided less identity certainty. Thus, the Task Force argued that the attribute certificate needed to be available for those agencies requirinf this highly secure approach, but that it would not be mandatory for any agency to use these attribute certificates. Additionally, vendors questioned whether it was necessary to make attribute certificates confidential since certificates are generally public. The Biometric Task Force responded that some of the data in the attribute certificates should be protected and that attribute certificates allow for encryption of data portions.

Several vendors suggested that more specific biometric requirements for each biometric type be added to the biometric section. The Biometrics Task Force resisted the request for additional specificity, arguing that the goal was to provide adequate functional requirements without being so specific as to limit the ability of vendors to propose innovative solutions. Consequently, the requirements document will not be revised to reflect greater specificity. Individual agencies may, however, provide their own specific requirements.

Requiring multi-factor biometrics was suggested as a means to reduce errors and provide for a more secure identification of the individual. The Biometric Task Force responded that there is no reason a 2-factor biometric system could not be proposed to meet the requirements contained in the current requirements document. As long as the 2-factor template is a reasonable size to be stored on the card, the currently specified storage methods should work. The Task Force rejected the idea of making the 2-factor biometric a mandatory requirement because not all agencies or applications may require the increased security and cost of such an approach.

Technology

Vendors questioned the practicality of mandating both the contactless chip and cryptographic capability, as cards with such capabilities are more difficult and expensive to obtain. As many agencies already have expressed the need for cards with such capabilities, the Advisory Group determined that the requirements document would remain unchanged in this regard. Although vendors must make these capabilities available, they need not be obtained by agencies.

The concern over interoperability prompted some vendors to question whether agencies should be allowed to specify card and reader specs or should they only be able to add optional requirements on to a common core spec. The issue of specificity was raised in yet other contexts. For example, in order to accommodate advances in technology, many vendors suggested less specificity in workstation specs, as well as physical access control system configurations. One vendor argued against inclusion of the specific approach to database backup provided in the document, requesting that alternative approaches be considered.

While some vendors argued for less specificity, others were proponents of greater technical definition, suggesting that a single operating system be mandated or that standard data structures, precise data formats, passwords or keys to access data, and applet selection processes be better defined. In many instances, the Advisory Group favored flexibility. The Advisory Group stressed that agencies must be allowed to balance their own unique requirements with reduced interoperability. Reducing the specificity, the Advisory Group argued, should also encourage alternative approaches to be proposed and reduce the possibility of precluding any potential solutions. To address these concerns, the Advisory Committee recommended that the document be revised to reflect a greater emphasis on needed functionality rather than on specific designs for implementation.

A number of vendors requested the addition of specific technologies. For example, vendors suggested that requirements for memory cards, secure access modules, and intelligent card acceptance devices be added to the document. Additionally, vendors requested increased discussion of role-based access control.

Security

Vendors questioned the practicality of some technical requirements to enhance security. For example, it was pointed out that few vendors could presently show that their Cryptographic Module Protection is in conformance with FIPS-140-1 and that it would be both expensive and time consuming to have to prove this compliance. Similarly, vendors questioned whether servers and workstations should be required to execute a FIPS 140-1 compliant operating environment. Generally, the Advisory Group favored maintaining the questioned requirements as a means to encourage industry to move in the desired direction of enhanced security.

Several vendors debated the degree of transaction auditing needed for a secure system. Some vendors favored capturing all accesses to cardholder data for audit, while other vendors argued that such an approach would be impractical because it would require such a great number of audit events. The Advisory Group determined that this requirement should be specified at the agency level, as long as government-wide audit statements are not contradicted.

Another area of concern was that the document should address different authentication requirements for different card applications. It was pointed out that the document needed to specify that graded or multi-level access control mechanisms, as well as secure file sharing capabilities were needed for this card platform. The Advisory Group agreed that a general statement about such security objectives should be incorporated in the document, but that particular approaches to achieving these objectives should not be specified.

Interoperability

Of all of the issues, interoperability was probably the most contentious. Many of the detailed comments received from vendors were in some way related to the issue of interoperability. One vendor questioned whether it was practical to cite interoperability as a requirement at all, considering the problematic nature of achieving interoperability at this point in time. Other vendors expressed reservations about whether interoperability could practically be achieved without detailed technical specifications. Still other vendors questioned which vendors, primary or secondary or both, should be held responsible for interoperability. It was suggested that an entity be established to manage the passwords and keys across applications to ensure interoperability while maintaining overall integrity and security of each issuer’s card structure and the overall card framework for GSA.

The Advisory Group expended substantial time in the discussion of interoperability issues. While the members of the Advisory Group understand that only limited interoperability may be possible at this time, they wish to encourage and support interoperability to the extent it can be achieved in the current technological environment. GSA will champion any industry efforts (such as have occurred in the travel and entertainment industry) to refine existing standards, as well as to define common data structures or application standards to promote interoperability across agencies. Furthermore, GSA will actively encourage agencies for which achieving interoperability with other agencies is a high priority, to develop interagency agreements to support such interoperability prior to issuing their individual task orders under the Smart Access Common ID Card contract vehicle. To promote interoperability and assist the individual agencies in their smart card implementations, GSA will develop administrative guidelines and conduct pilots to explore alternative models for achieving interoperability.

Business Case

Many vendors were concerned about the underlying business case supporting the Smart Access Common ID Card RFP. One vendor suggested that a business case should be part of the requirements document, while another vendor requested that GSA limit the award only to a few vendor teams in order to ensure a viable business case. It was suggested that GSA guarantee minimum volumes for each team on the contract.

The Advisory Group agreed that it would be inappropriate to address the business case within a requirements document. While GSA would be unwilling to guarantee minimum volumes, it would encourage the concept of tiered pricing. Furthermore, GSA will actively market the Smart Access Common ID Card contract to the agencies and provide guidelines for those agencies planning implementations under this contracting vehicle.